| | |
|---|---|
| **REPORT DOCUMENTATION PAGE** | *Form Approved*<br>**OMB No. 0704-0188** |

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Service, Directorate for Information Operations and Reports,
1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget,
Paperwork Reduction Project (0704-0188) Washington, DC 20503.
**PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

| | | |
|---|---|---|
| 1. REPORT DATE *(DD-MM-YYYY)*<br>15-11-2010 | 2. REPORT TYPE<br>Quarterly technical report | 3. DATES COVERED *(From - To)*<br>11 August 2010 - 14 Nov 2010 |

| | |
|---|---|
| 4. TITLE AND SUBTITLE<br>Integrated Social and QoS Trust-Based Routing in Mobile Ad Hoc Delay Tolerant Networks | 5a. CONTRACT NUMBER |
| | 5b. GRANT NUMBER<br>N00014-10-1-0156 |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S)<br>Chen, Ing-Ray (VT)<br>Bao, Fenye (VT)<br>Chang, Moonjeong (VT)<br>Cho, Jin-Hee (ARL) | 5d. PROJECT NUMBER<br>10PR02543-01 |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |

| | |
|---|---|
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br>VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY<br>OFFICE OF SPONSORED PROGRAMS<br>1880 PRATT DRIVE, SUITE 2006<br>BLACKSBURG, VA 24060-3325 | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)<br>Office of Naval Research<br>875 North Randolph Street<br>Arlington, VA 22203-1995 | 10. SPONSOR/MONITOR'S ACRONYM(S)<br>ONR |
| | 11. SPONSORING/MONITORING AGENCY REPORT NUMBER |

12. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

We propose and analyze a class of integrated social and quality of service (QoS) trust-based routing protocols in mobile ad-hoc delay tolerant networks. The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only QoS trust properties but also social trust properties to evaluate other nodes encountered. We prove that our protocol is resilient against bad-mouthing, good-mouthing and whitewashing attacks performed by malicious nodes. By utilizing a stochastic Petri net model describing a delay tolerant network consisting of heterogeneous mobile nodes with vastly different social and networking behaviors, we analyze the performance characteristics of trust-based routing protocols in terms of message delivery ratio, message delay, and message overhead against epidemic routing and connectivity-based routing protocols. The results indicate that our trust-based routing protocols can approach the ideal performance obtainable by epidemic routing in delivery ratio and message delay, without incurring high message overhead. Further, integrated social and QoS trust-based protocols can effectively trade off message delay and message overhead for a significant gain in message delivery ratio over traditional connectivity-based routing protocols.

15. SUBJECT TERMS
Mobile ad hoc networks, delay tolerant networks, trust management, trust-based routing, social networks, resiliency, performance analysis, stochastic Petri nets.

| | | | |
|---|---|---|---|
| 16. SECURITY CLASSIFICATION OF: | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON<br>Chen, Ing-Ray |

20101118006

INSTRUCTIONS FOR COMPLETING SF 298

| | | | | | |
|---|---|---|---|---|---|
| a. REPORT<br>U | b. ABSTRACT<br>U | c. THIS PAGE<br>U | SAR | 6 | 19b. TELEPONE NUMBER (*Include area code)*<br>(703) 538-8376 |

INSTRUCTIONS FOR COMPLETING SF 298

**1. REPORT DATE.** Full publication date, including day, month, if available. Must cite at lest the year and be Year 2000 compliant, e.g., 30-06-1998; xx-08-1998; xx-xx-1998.

**2. REPORT TYPE**. State the type of report, such as final, technical, interim, memorandum, master's thesis, progress, quarterly, research, special, group study, etc.

**3. DATES COVERED**. Indicate the time during which the work was performed and the report was written, e.g., Jun 1997 - Jun 1998; 1-10 Jun 1996; May - Nov 1998; Nov 1998.

**4. TITLE.** Enter title and subtitle with volume number and part number, if applicable. On classified documents, enter the title classification in parentheses.

**5a. CONTRACT NUMBER**. Enter all contract numbers as they appear in the report, e.g. F33615-86-C-5169.

**5b. GRANT NUMBER.** Enter all grant numbers as they appear in the report, e.g. 1F665702D1257.

**5c. PROGRAM ELEMENT NUMBER.** Enter all program element numbers as they appear in the report, e.g. AFOSR-82-1234.

**5d. PROJECT NUMBER.** Enter al project numbers as they appear in the report, e.g. 1F665702D1257; ILIR.

**5e. TASK NUMBER.** Enter all task numbers as they appear in the report, e.g. 05; RF0330201; T4112.

**5f. WORK UNIT NUMBER.** Enter all work unit numbers as they appear in the report, e.g. 001; AFAPL30480105.

**6. AUTHOR(S).** Enter name(s) of person(s) responsible for writing the report, performing the research, or credited with the content of the report. The form of entry is the last name, first name, middle initial, and additional qualifiers separated by commas, e.g. Smith, Richard, Jr.

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES).** Self-explanatory.

**8. PERFORMING ORGANIZATION REPORT NUMBER.** Enter all unique alphanumeric report numbers assigned by the performing organization, e.g. BRL-1234; AFWL-TR-85-4017-Vol-21-PT-2.

**9. SPONSORING/MONITORS AGENCY NAME(S) AND ADDRESS(ES).** Enter the name and address of the organization(s) financially responsible for and monitoring the work.

**10. SPONSOR/MONITOR'S ACRONYM(S).** Enter, if available, e.g. BRL, ARDEC, NADC.

**11. SPONSOR/MONITOR'S REPORT NUMBER(S).** Enter report number as assigned by the sponsoring/ monitoring agency, if available, e.g. BRL-TR-829; -215.

**12. DISTRIBUTION/AVAILABILITY STATEMENT.** Use agency-mandated availability statements to indicate the public availability or distribution limitations of the report. If additional limitations/restrictions or special markings are indicated, follow agency authorization procedures, e.g. RD/FRD, PROPIN, ITAR, etc. Include copyright information.

**13. SUPPLEMENTARY NOTES.** Enter information not included elsewhere such as: prepared in cooperation with; translation of; report supersedes; old edition number, etc.

**14. ABSTRACT.** A brief (approximately 200 words) factual summary of the most significant information.

**15. SUBJECT TERMS.** Key words or phrases identifying major concepts in the report.

**16. SECURITY CLASSIFICATION.** Enter security classification in accordance with security classification regulations, e.g. U, C, S, etc. If this form contains classified information, stamp classification level on the top and bottom of this page.

**17. LIMITATION OF ABSTRACT.** This block must be completed to assign a distribution limitation to the abstract. Enter UU (Unclassified Unlimited) or SAR (Same as Report). An entry in this block is necessary if the abstract is to be limited.

# Integrated Social and QoS Trust-Based Routing in Mobile Ad Hoc Delay Tolerant Networks

Ing-Ray Chen, Fenye Bao, Moonjeong Chang
Department of Computer Science
Virginia Tech
{irchen, baofenye, mjchang}@vt.edu

Jin-Hee Cho
Computational and Information Sciences
U.S. Army Research Laboratory
jinhee.cho@us.army.mil

**Abstract**: We propose and analyze a class of integrated social and quality of service (QoS) trust-based routing protocols in mobile ad-hoc delay tolerant networks. The underlying idea is to incorporate trust evaluation in the routing protocol, considering not only *QoS trust* properties but also *social trust* properties to evaluate other nodes encountered. We prove that our protocol is resilient against bad-mouthing, good-mouthing and whitewashing attacks performed by malicious nodes. By utilizing a stochastic Petri net model describing a delay tolerant network consisting of heterogeneous mobile nodes with vastly different social and networking behaviors, we analyze the performance characteristics of trust-based routing protocols in terms of message delivery ratio, message delay, and message overhead against epidemic routing and connectivity-based routing protocols. The results indicate that our trust-based routing protocols can approach the ideal performance obtainable by epidemic routing in delivery ratio and message delay, without incurring high message overhead. Further, integrated social and QoS trust-based protocols can effectively trade off message delay and message overhead for a significant gain in message delivery ratio over traditional connectivity-based routing protocols.

**Keywords:** Delay tolerant networks, opportunistic routing, trust management, trust-based routing, social networks, resiliency, performance analysis, stochastic Petri nets.

## 1. Introduction

A delay tolerant network (DTN) provides interoperable communications through mobile nodes with the characteristics of high end-to-end path latency, frequent disconnection, limited resources (e.g., battery, computational power, bandwidth), and unreliable wireless transmission.

Further, for DTNs in mobile ad hoc network (MANET) environments, we also face additional challenges due to a lack of centralized trusted entity and this increases security vulnerability [5]. For a sparse MANET DTN, mobility-assisted routing based on *store-carry-and-forward* method has been used. That is, a message carrier forwards a message to an encountered node until the message reaches a destination node. In MANET DTN environments, it is important to select a trustworthy node as a next message carrier among all encountered nodes to minimize the delay for a message to reach a destination node as well as to maximize the message delivery ratio. In this paper, we consider a MANET DTN in the presence of selfish and malicious nodes and propose a family of trust-based routing protocols to select a highly trustworthy next message carrier with the goal of maximizing the message delivery ratio without incurring a high delay or a high message overhead.

In the literature, DTN routing protocols based on encounter patterns have been investigated [2, 10, 11]. However, if the predicted encounter does not happen, then messages would be lost for single-copy routing, or flooded for multi-copy routing. Moreover, these approaches could not guarantee reliable message delivery due to the presence of selfish or malicious nodes. The vulnerability of DTN routing to node selfishness was well studied in [7]. Several recent studies [12, 14, 15] considered using reputation in selecting message carriers among encountered nodes for DTNs. Nevertheless, [12, 14] assumed that a centralized entity exists for credit management, and [15] merely used reputation to judge if the system should switch from reputation-based routing to multipath routing when many selfish nodes exist.

There is very little research to date on the social aspect of trust management for DTN routing. Social relationship and social networking were considered as criteria to select message carriers in a MANET DTN [6, 8]. However, no consideration was given to the presence of malicious or selfish nodes. Very recently, [9] considered routing by socially selfish nodes in DTNs, taking into consideration the willingness of a socially selfish node to forward messages to the destination node because of social ties. Unlike prior work cited above, in this paper, we integrate *social trust* and *Quality of Service (QoS) trust* into a composite trust metric for determining the best node among the new encounters for message forwarding. We consider *honesty* and *unselfishness* for social trust to account for a node's trustworthiness for message delivery, and *connectivity* for QoS trust to account for a node's capability to quickly deliver the message to the destination node. By assigning various weights associated with these QoS and social trust properties, we form a class of DTN routing protocols, from which we examine two versions of the trust management protocol in this paper: an equal-weight QoS and social trust management protocol (called trust-based routing for short) and a QoS trust only management protocol (called connectivity-based routing for short). We analyze and compare the performance characteristics of trust-based routing and connectivity-based routing protocols with epidemic routing [13] for a DTN consisting of heterogeneous mobile nodes with vastly different social and networking behaviors. The results indicate that our trust-based routing protocol approaches the ideal performance of epidemic routing in delivery ratio, while connectivity-based routing approaches the ideal performance of epidemic routing in message delay, as the percentage of selfish and malicious nodes present in the DTN system increases. All DTN routing protocols in the class significantly outperform epidemic routing in message overhead.

## 2. System Model

We consider a MANET DTN environment with no centralized trusted authority. Nodes communicate through multi-hops. Every node may have a different level of energy and speed reflecting node heterogeneity. We differentiate selfish nodes from malicious nodes. A selfish node acts for its own interest. So it may drop packets arbitrarily just to save energy but it may decide to forward a packet if it has good social ties with the destination node. A malicious node acts maliciously with the intention to disrupt the main functionality of the DTN, so it can drop packets, jam the wireless channel, perform bad-mouthing attacks (provide negative recommendations against good nodes), perform good-mouthing attacks (provide positive recommendations for other colluding malicious nodes) and even forge packets. To deal with malicious nodes, we assume that a distributed intrusion detection system (IDS) exists for detecting malicious nodes. As soon as a malicious node is detected by IDS, the malicious node will be made known to all nodes, which will set the trust value of the malicious node to zero and thus exclude it as a message carrier for message forwarding. Since there is no perfect IDS, we characterize the distributed IDS by its false positive and false negative probabilities for which less than 1% is deemed acceptable. We also assume that a malicious node is always bad until it is detected by IDS. In the paper, we will use the terms a malicious node, a compromised node, and a bad node interchangeably.

We consider the following model to describe a node's behaviors. If a node is selfish, the speed of energy consumption is slowed down and vice versa. If a node is compromised but not detected by IDS, the speed of energy consumption will increase since the node may have a chance to perform attacks which may consume more energy, e.g., disseminating bogus messages. We also consider redemption mechanism for a selfish node to have a second chance. That is, a selfish node may become unselfish again, especially when its energy is still high compared with its peers.

A node's trust value is assessed based on direct observations and indirect information like recommendations. The trust of one node toward another node is updated upon encounter events. Our trust metric consists of two trust types: *QoS trust* and *social trust*. *QoS trust* is evaluated through the communication by the capability of a node to deliver messages to the destination node. We consider ***connectivity*** to measure the QoS trust level of a node. Social trust is based on social relationships. We consider ***unselfishness*** and ***honesty*** to measure the social trust level of a node. Different from most existing encounter-based routing protocols which considered only connectivity, we consider social trust in addition to QoS trust in order to select more trustworthy message carriers among encountered nodes. It is worth noting that unselfishness traditionally has been considered as a QoS trust metric [3] to measure the extent to which a node cooperates with other nodes to conform to protocol execution. Here we consider unselfishness as a social trust metric to measure if a node is socially willing to route packets passed to it in a DTN, thereby modeling the social behavior exhibited by a selfish node. We define a node's trust level as a real number in the range of [0, 1], with 1 indicating complete trust, 0.5 ignorance, and 0 complete distrust.

## 3. Trust Management for Message Routing

The trust value of node *j* as evaluated by node *i* at time *t*, denoted as $T_{i,j}(t)$, is computed by a weighted average of connectivity, honesty, and unselfishness trust components. Specifically node *i* will compute $T_{i,j}(t)$ by:

$$T_{i,j}(t) = w_1\, T_{i,j}^{e-connectivity}(t) + w_2\, T_{i,j}^{d-connectivity}(t) + w_3\, T_{i,j}^{honesty}(t) + w_4\, T_{i,j}^{unselfishness}(t) \quad (1)$$

where $w_1{:}w_2{:}w_3{:}w_4$ is the weight ratio with $w_1 + w_2 + w_3 + w_4 = 1$. Of these trust components (or properties) in Equation 1, $T_{i,j}^{e-connectivity}(t)$ is about node *i*'s belief in node *i*'s encounter connectivity to node *j*, representing the delay of node *i* passing the message to node *j*, $T_{i,j}^{d-connectivity}(t)$ is about node *i*'s belief in node *j*'s connectivity to the destination node *d*, representing the delay of node *j* passing the message to node *d*, $T_{i,j}^{honesty}(t)$ is about node *i*'s belief in node *j*'s honesty, and $T_{i,j}^{unselfishness}(t)$is about node *i*'s belief in node *j*'s unselfishness. In message forwarding in DTNs, two most important performance metrics are message delivery ratio and delay. The rationale of using these four trust metrics is to rank nodes such that high $T_{i,j}^{e-connectivity}(t)$ and $T_{i,j}^{d-connectivity}(t)$ represent low delay, while high $T_{i,j}^{honesty}(t)$ and $T_{i,j}^{unselfishness}(t)$ represent high delivery ratio. We set $T_{i,j}^{e-connectivity}(0)$, $T_{i,j}^{d-connectivity}(0)$, $T_{i,j}^{honesty}(0)$ and $T_{i,j}^{unselfishness}(0)$ to ignorance (0.5) since initially there is no information exchanged among nodes.

We define a minimum trust threshold $T_{min}$ also set to ignorance (0.5) such that if $T_{i,j}(t) > T_{min}$, node *i* will consider node *j* as "trustworthy" (or plainly as a good node) at time *t*. When node *i* encounters another node, say node *m*, it exchanges its encounter history with node *m*. Moreover, if node *i* believes that node *m* is a good node, i.e., $T_{i,m}(t + \Delta t) > T_{min}$, node *i* will use node *m* as a recommender to update its beliefs toward other nodes. Specifically, node *i* will update its trust toward node *j* upon encountering node *m* at time *t* for a duration of $\Delta t$ as follows:

$$T_{i,j}^{X}(t + \Delta t) = \beta_1\, T_{i,j}^{direct,\ X}(t + \Delta t) + \beta_2\, T_{i,j}^{indirect,\ X}(t + \Delta t) \tag{2}$$

Here *X* refers to a trust property (e-connectivity, d-connectivity, honesty, or unselfishness) with:

$$T_{i,j}^{direct,\ X}(t + \Delta t) = \begin{cases} T_{i,m}^{encounter,X}(t + \Delta t), if\ m = j \\ T_{i,j}^{X}(t), if\ m \neq j \end{cases} \tag{3}$$

$$T_{i,j}^{indirect,\ X}(t + \Delta t) = \begin{cases} T_{i,m}^{X}(t), if\ m = j \\ T_{i,j}^{X}(t), if\ m \neq j\ and\ T_{i,m}(t + \Delta t) \leq T_{min} \\ T_{i,m}^{X}(t + \Delta t) \times T_{m,j}^{X}(t + \Delta t), if\ m \neq j\ and\ T_{i,m}(t + \Delta t) > T_{min} \end{cases} \tag{4}$$

In Equation 2, $\beta_1$ is a weight parameter to weigh node *i*'s own trust assessment toward node *j* at time $t + \Delta t$, i.e., "self-information," and $\beta_2$ is a weight parameter to weigh indirect information from the recommender, i.e., "other-information," with $\beta_1 + \beta_2 = 1$. In Equation 3 for the direct trust calculation of node *j*, if the new encounter (node $m$) is node *j* itself, then node *i* can directly evaluate node *j*. We use $T_{i,m}^{encounter,X}(t + \Delta t)$ to denote the assessment result of node *i* toward node $m$ in trust property *X* based on node *i*'s past experiences with node $m$ up to time $t + \Delta t$. Later in Section 4, we will describe how this can be obtained. If the new encounter is not node *j*, then no new direct information can be gained about node *j*, so node *i* will just use its past trust toward node *j* obtained at time *t*. In Equation 4 for the indirect trust calculation of node *j*, if the new encounter is node *j* itself, then there is no indirect recommendation for node *j*, so node *i* will just use its past trust obtained at time *t*. If the new encounter is not node *j*, then node $m$ can provide its recommendation to node *i* for evaluating node *j*, if node *i* considers node $m$ as trustworthy, i.e., $T_{i,m}(t + \Delta t) > T_{min}$. In this case, we must take into account node *i*'s belief in node $m$ in the calculation of $T_{i,j}^{indirect,\ X}(t + \Delta t)$. This models the decay of trust as trust is derived from a distant node as indirect information. On the other hand, if node *i* does not consider node $m$ as a good node because of $T_{i,m}(t + \Delta t) \leq T_{min}$, then node *i* refuses to take recommendations from node $m$ about node *j*, and will just use its past trust information about node *j* obtained at time *t*. The policy that recommendations from a newly encounter node are accepted only if the newly encountered node is considered a good node provides robustness against bad-mouthing or good-mouthing attacks.

$T_{i,j}(t)$ in Equation 1 can be used by node *i* (if it is a message carrier) to decide, upon encountering node *m*, if it should forward the message to node *m* with the intent to shorten the message delay or improve the message delivery ratio. We consider a **Ω**–permissible policy in this paper, i.e., node *i* will pass the message to node *m* if $T_{i,m}(t)$ is in the top **Ω** percentile among all $T_{i,j}(t)'s$. We experiment with various values of **Ω** to trade message delivery ratio with message latency.

## 4. Protocol Resiliency

Below we provide a formal proof that our trust management protocol is resilient against malicious attacks, including whitewashing attacks (a bad node washing away its bad reputation by gaining high trust upon encountering with another node), bad-mouthing attacks (a bad node providing bad recommendations toward a good node to ruin its reputation), and good-mouthing attacks (a bad node providing good recommendations for a colluding bad node to raise its reputation).

### 4.1 Resiliency to Whitewashing Attacks

*Definition 1:* A bad node, say node *m*, upon encountering node *i* at time *t* for an encounter interval $\Delta t$, is said to perform a whitewashing attack successfully against node *i* if $T_{i,m}(t) \leq T_{min}$ and $T_{i,m}(t + \Delta t) > T_{min}$.

*Lemma 1: Our protocol is resilient against whitewashing attacks.*

*Proof:* When node *i* encounters node *m* at time *t* for a duration of $\Delta t$, according to our protocol $T_{i,m}(t + \Delta t) = \beta_1 T_{i,m}^{encounter}(t + \Delta t) + \beta_2 T_{i,m}(t)$, of which $T_{i,m}(t) \leq T_{min}$ is given (in the *if* part) and $T_{i,m}^{encounter}(t + \Delta t) \leq T_{min}$ is true because node *i* will be able to observe node *m*'s bad behavior directly based on node *i*'s past experiences with node *m* up to time $t + \Delta t$, including the current encounter. Taking the fact that $\beta_1 + \beta_2 = 1$, we obtain $T_{i,m}(t + \Delta t) \leq T_{min}$. Thus, it is impossible that a bad node can successfully perform a whitewashing attack.

### 4.2 Resiliency to Bad-Mouthing Attacks

*Definition 2:* A bad node, say node *m*, upon encountering node *i* at time *t* for an encounter interval $\Delta t$, is said to perform a bad-mouthing attack successfully against a good node, say node *j*, if $T_{i,j}(t) > T_{min}$ and $T_{i,j}(t + \Delta t) \leq T_{min}$.

*Lemma 2: Our protocol is resilient against bad-mouthing attacks.*

*Proof:* The proof hinges on proving $T_{i,m}(t + \Delta t) \leq T_{min}$ and therefore node *i* will refuse to take recommendations from node *m* about node *j*. Utilizing the proof to Lemma 1 and the fact that $T_{i,m}(t) \leq T_{min}$ is true (because we set the initial trust value to ignorance, i.e., $T_{i,m}(0) = T_{min}$, making it impossible for a bad node to gain trustworthy status at time *t*), we know $T_{i,m}(t + \Delta t) \leq T_{min}$ is true. Consequently, node *i* will not take recommendations from node *m* about node *j*. According to our protocol, $T_{i,j}(t + \Delta t) = \beta_1 T_{i,j}(t) + \beta_2 T_{i,j}(t)$. This leads to $T_{i,j}(t + \Delta t) > T_{min}$ because $\beta_1 + \beta_2 = 1$ and $T_{i,j}(t) > T_{min}$ is given (in the *if* part). Therefore, it is impossible that a bad node can successfully perform a bad-mouthing attack.

### 4.3 Resiliency to Good-Mouthing Attacks

*Definition 3:* A bad node, say node *m*, upon encountering node *i* at time *t* for an encounter interval $\Delta t$, is said to perform a good-mouthing attack successfully for a bad node, say node *k*, if $T_{i,k}(t) \leq T_{min}$ and $T_{i,k}(t + \Delta t) > T_{min}$.

*Lemma 3: Our protocol is resilient against good-mouthing attacks.*

*Proof:* Following the proof to Lemma 2, we know that $T_{i,m}(t + \Delta t) \leq T_{min}$ is true. Hence, node *i* refuses to take recommendations from node *m* about node *k* and $T_{i,k}(t + \Delta t) = \beta_1 T_{i,k}(t) + \beta_2 T_{i,k}(t)$ according to our protocol. This leads to $T_{i,k}(t + \Delta t) \leq T_{min}$ because $\beta_1 + \beta_2 = 1$ and $T_{i,k}(t) \leq T_{min}$ is given (in the *if* part). Therefore, it is impossible that a bad node can successfully perform a good-mouthing attack.

## 5. Performance Model

We analyze the performance of the proposed trust-based routing protocol for DTN message forwarding by a probability model based on stochastic Petri net (SPN) techniques [4] due to its ability to handle a large number of states. The SPN model is shown in Figure 1. The SPN model describes a node's lifetime in the presence of selfish and malicious nodes, and IDS for detecting malicious nodes. It is used to obtain each node's information (e.g., connectivity, honesty, and unselfishness) and to derive the trust relationship with other nodes in the system. Without loss of generality, we consider a square-shaped operational area consisting of *m*×*m* sub-grid areas with the width and height equal to the radio range (*R*). Initially nodes are randomly distributed over the operational area based on uniform distribution. A node randomly moves to one of four locations in four directions (i.e., north, west, south, and east) in accordance with its mobility rate. To avoid end-effects, movement is wrapped around (i.e., a torus is assumed). The SPN model produces the probability that node *i* is in a particular location *L* at time *t*. This information along with the location information of other nodes at time *t* provides us the probability of two nodes encountering with each other, and how often two nodes exchange encounter histories to update $T^{X}_{i,j}(t)$.

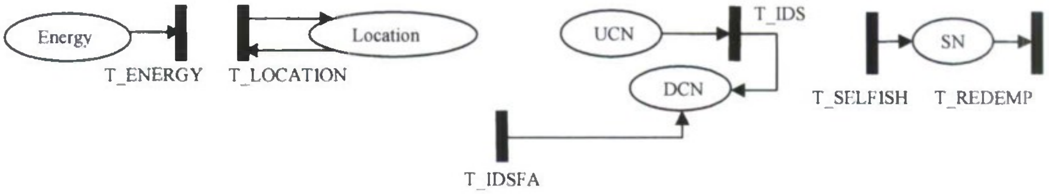


**Figure 1: SPN Model.**

Below we explain how we construct the SPN model for describing a node's behavior in terms of its location, energy level, degree of honesty (e.g., whether or not a node is compromised or/and detected by IDS), and degree of selfishness.

**Location**: Transition T_LOCATION is triggered when the node moves to a randomly selected area out of four different directions from its current location with the rate calculated as $\sigma(t)/R$ based on its speed σ($t$) at time $t$ and wireless radio range ($R$). The speed at time $t$ is linearly proportional to its remaining energy, calculated as $\sigma_0 \times E_{remain} / E_0$ where $\sigma_0$ is the initial speed, $E_0$ is the initial energy and $E_{remain}$ is the remaining energy given by *mark(Energy)*.

**Connectivity**: Connectivity of node $j$ to the destination node $d$ is measured by the time-averaged probability that node $j$ and node $d$ are within one-hop during [$t$-$n\Delta t$, $t$], modeling not only chances, but also recency of encountering events between node $j$ and node $d$. This can be obtained by knowledge of location probabilities of node $j$ and node $d$ during [$t$-$n\Delta t$, $t$].

**Energy**: Place *Energy* represents the current energy level of a node. An initial energy level of each node is assigned according to node heterogeneity information. A token is taken out when transition T_ENERGY fires. The transition rate of T_ENERGY is adjusted on the fly based on a node's state. It is lower when a node is selfish to save energy; it is higher when the node is compromised so that it performs attacks more and consumes energy more. We use the energy model in [3] to adjust the rate to consume one token in place *Energy* based on a node's state.

**Honesty**: If the node is compromised, a token goes to *UCN*, meaning that the node is already compromised but not yet detected by IDS. While the node is not detected by IDS, it has a chance to perform attacks. If a compromised node is detected by IDS, a token is taken out from *UCN* into *DCN* and the node is evicted immediately. We model a MANET DTN equipped with IDS characterized by false alarm probabilities. A false negative probability ($P_{fn}^{IDS}$) of IDS is considered in T_IDS which has the rate of $\left(1 - P_{fn}^{IDS}\right)/T_{IDS}$ and a false positive probability ($P_{fp}^{IDS}$) of IDS is considered in T_IDSFA which has the rate of $P_{fp}^{IDS}/T_{IDS}$.

**Selfishness**: Place *SN* represents whether a node is selfish or not. If a node becomes selfish, a token goes to *SN* by triggering T_SELFISH. We model a node's selfish behavior as a function of its remaining energy. Specifically, the transition rate to T_SELFISH is given by:

$$rate(T\_SELFISH) = \frac{f(E_{remain})}{\Delta t} \tag{5}$$

where $\Delta t$ is the duration between two encountering events over which a node may decide to become selfish. The form $f(y) = \alpha_1 y^{-\varepsilon_1}$ follows the demand-pricing relationship in Economics [1] to model the effect of its argument $y$ on the selfishness behavior, such that $f(E_{remain})$ models the behavior that a node with a higher level of energy is less likely to be selfish. Similarly a selfish node may become unselfish again through transition T_REDEMP. The redemption rate is modeled in a similar way as:

$$rate(T\_REDEMP) = \frac{g(E_{consumed})}{\Delta t} \tag{6}$$

where $g(y) = \alpha_2 y^{-\varepsilon_2}$ and $E_{consumed}$ is the amount of energy consumed as given by $E_0 - E_{remain}$and $\Delta t$ is the encountering interval over which a selfish node may decide to become unselfish again. $g(E_{consumed})$ models the behavior that a node with a lower level of energy will more likely stay selfish to further save its energy considering its own individual benefit.

With the node behaviors modeled by the SPN model described above we can calculate $T_{i,j}^{X}(t)$ as follows. When node *i* encounters node *m*, node *i* will assess node *m* in trust property *X* to yield $T_{i,m}^{encounter,X}(t)$ based on its past experiences up to time *t*. Because node *i* has prior close interaction experiences with node *m* (including the current encounter), node *i* has good knowledge about whether node *m* is selfish or not through snooping and overhearing. Hence, node *i*'s direct assessment in node *m*'s selfishness at the encounter time *t* is the same as or close to the selfishness status of node *m* at time *t*. Consequently, $T_{i,m}^{encounter,\ unselfishness}(t)$ in Equation 3 is simply equal to the probability that place *SN* does not contain a token at time *t*, which we can compute easily from the SPN output. Similarly, node *i* can fairly accurately assess $T_{i,m}^{encounter,\ e-connectivity}(t)$ by consulting its encounter history with node *m* over $[t - n\Delta t, t]$

and $T_{i,m}^{encounter,\ d\text{-}connectivity}(t)$ by consulting all encounter histories it has over $[t - n\Delta t, t]$. These two quantities can be obtained by utilizing the SPN output regarding the node location probability at time *t*. For the honesty trust component, node *i* knows that node *m* is malicious only when IDS detects it and announces a message to the system, i.e., when node *m*'s place *DCN* (in Figure 1) is not zero. Thus, we can compute $T_{i,m}^{encounter,\ honesty}(t)$ by the probability that place *DCN* in node *m* does not contain any token at time *t*. Once $T_{i,m}^{encounter,X}(t)$ is obtained at each encounter time, node *i* can update its $T_{i,j}^{X}(t)$ based on Equation 2, and subsequently, can obtain $T_{i,j}(t)$ based on Equation 1.

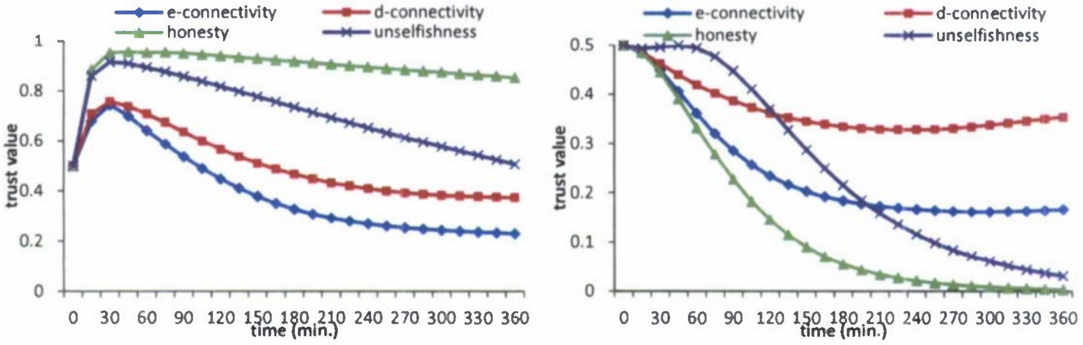
## 6. Results

**Table 1: Default parameter values used.**

| Param | Value | Param | Value | Param | Value | Param | Value |
|---|---|---|---|---|---|---|---|
| $m \times m$ | 8×8 | $R$ | 250*m* | $T_{IDS}$ | 600*s* | $\sigma_0$ | (0, 2] *m/s* |
| $\alpha_1$ | 4 | $\alpha_2$ | 0.5 | $\varepsilon_1$ | 1.6 | $\varepsilon_2$ | 1.6 |
| $P_{fn}^{IDS}, P_{fp}^{IDS}$ | 0.5% | $\Omega$ | 90% | $\Delta t$ | 300 *s* | $E_0$ | [12, 24] *hrs* |
| $\beta_1{:}\beta_2$ | 0.8:0.2 | $N$ | 2 | $T_{min}$ | 0.5 | | |

Below we show numerical results and provide physical interpretation of the results obtained. Table 1 lists the default parameter values used. For trust-based routing, we set $w_1 : w_2 : w_3 : w_4 = 0.25 : 0.25 : 0.25 : 0.25$ for e-connectivity: d-connectivity: honesty: unselfishness, while for connectivity-based routing, we set $w_1 : w_2 : w_3 : w_4 = 0.5 : 0.5 : 0 : 0$. We setup 20 nodes with vastly different initial energy levels in the system moving randomly in a 8×8 operational region with the mobility rate of each node proportional to the node's remaining energy in the range of (0, 2] *m/s*, and with each area covering 250 *m* radio radius. There are two sets of nodes, namely, good nodes and bad nodes, and we vary the percentage of bad nodes to test their effect on the performance of our protocol. A good node may become selfish to save energy and unselfish again after redemption, with the selfish rate defined based on Equation 5 and redemption rate defined by Equation 6. A good node can also be misdiagnosed by IDS as a bad node, in which case a token is put in place *DCN*. Bad nodes are compromised nodes with a token in place *UCN*. We use all encounters as the recommenders. The initial trust level is set to ignorance (i.e., 0.5) for all trust components since initially nodes do not know each other. We also set $T_{min}$ to 0.5 so that a node will take recommendations from a newly encountered node only when its trust level toward the newly encountered node exceeds ignorance.

To reveal which trust component might have a more dominant effect, we show $T_{i,j}^{e-connectivity}(t)$, $T_{i,j}^{d-connectivity}(t)$, $T_{i,j}^{honesty}(t)$ and $T_{i,j}^{unselfishness}(t)$ for node *i* (a good node) evaluating node *j* randomly picked. Other nodes exhibit similar trends and thus only one set of results is shown. Figure 2(a) is for the case in which node *j* is a good node. We see that all trust components exhibit the same trend. A good node initially picks up its trustworthy status (with its trust level greater than $T_{min}$) due to favorable direct evaluations by those nodes it encounters and interacts with, who in turn pass on their positive recommendations to other nodes they encounter. All trust component values then decline as time progresses. The honesty trust value decreases over time because there is a non-zero IDS false positive probability of misdiagnosing node *j* as a bad node. The unselfishness trust value declines over time because node *j* tends to become more selfish as more energy is consumed. Lastly the e-connectivity and d-connectivity trust values also decline over time due to the fact that node *j* moves slower as more energy is consumed. Among all trust components, the honesty trust component is expected to contribute the most to the trustworthy status of a good node. This is reflected in Figure 2(a) which shows honesty dominates other trust components.



(a) Node *j* is a good node.

(b) Node *j* is a bad node.

**Figure 2: Comparing $T_{i,j}^{X}(t)$ as a function of time.**

Figure 2(b) shows $T_{i,j}^{e-connectivity}(t)$, $T_{i,j}^{d-connectivity}(t)$, $T_{i,j}^{honesty}(t)$ and $T_{i,j}^{unselfishness}(t)$ as a function of time for the case in which node *j* is a bad node. Here again all trust components exhibit the same trend. However, the trust values decrease monotonically over time. Contrary to a good node, a bad node never has any chance to attain trustworthy status, with the rapid decline of honesty and unselfishness especially contributing to a bad node's trust decline. The result that a bad node's status is always untrustworthy as demonstrated in Figure 2(b) substantiates our claim that our protocol is resilient against whitewashing, bad-mouthing, and good-mouthing attacks by malicious nodes.

Next we consider a message forwarding scenario in which in each run we randomly pick a source node *s* and a destination node *d*. The source and destination nodes picked are always good nodes. There is only a single copy of the message initially given to node *s*. We let the system run for 30 min. to warm up the system and start the message forwarding afterward in each run. During a message-passing run, every node *i* updates its $T_{i,j}(t)$ for all *j's* based on Equation 1. In particular, the current message carrier uses $T_{i,j}(t)$ to judge if it should pass the message to a node it encounters at time *t*. If the message carrier is malicious, the message is dropped (a weak attack). If the message carrier is selfish, the message delivery continues with 50% of the chance. A message delivery run is completed when the message is delivered to the destination node, or the message is lost before it reaches the destination node. Data are collected for 1500 runs from which the message delivery ratio, delay and overhead performance measurements are calculated.

Figure 3 shows the message delivery ratio as a function of the percentage of compromised and selfish nodes in the MANET DTN for trust-based and connectivity-based routing protocols. For performance comparison, we also show the delivery ratio obtained from epidemic routing. Here we see that trust-based routing outperforms connectivity-based routing in delivery ratio and its performance approaches the maximum achievable performance obtainable from epidemic routing. This is attributed to the ability of trust-based protocols being able to differentiate trustworthy nodes from selfish and bad nodes and select trustworthy nodes to relay the message. The result demonstrates the effectiveness of incorporating social trust into the decision making process for DTN message routing.

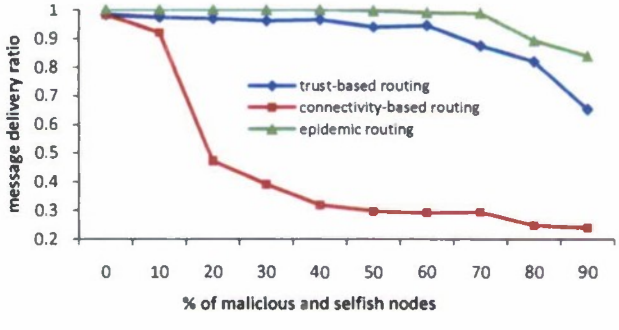


**Figure 3: Message delivery ratio: trust-based vs. connectivity-based and epidemic protocols.**

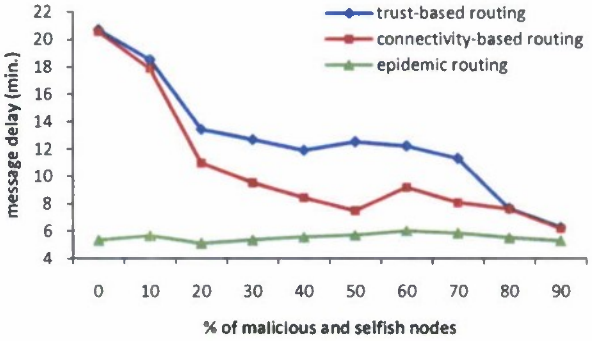


**Figure 4: Message delay: trust-based vs. connectivity-based and epidemic routing protocols.**

Figure 4 shows the average delay experienced per message considering only those messages delivered successfully. Here we first note that connectivity-based routing will always perform better than trust-based routing because connectivity-based protocols use the delay to encounter the next message carrier (e-connectivity) and the delay for the next message carrier to encounter the destination node (d-connectivity) as the criteria to select a message carrier. The result suggests that if delay is of primary concern, we should set the weights associated with e-connectivity and d-connectivity (QoS trust metrics) higher than those for honesty and unselfishness (social trust metrics), as connectivity-based routing does (by setting $w_1 : w_2 : w_3 : w_4 = 0.5 : 0.5 : 0 : 0$). This will have the effect of trading off high delivery ratio for low delay. Figure 4 also shows that connectivity-based routing approaches the ideal performance obtainable from epidemic routing as the percentage of malicious and selfish nodes increases.

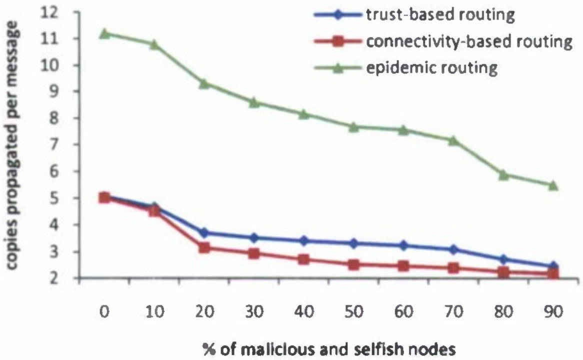


**Figure 5: Number of copies propagated per message.**

Figure 5 compares the three protocols in message overhead measured by the number of copies forwarded to reach the destination node for those messages successfully delivered. We see that trust-based protocols perform comparably with connectivity-based protocols and both protocols outperform epidemic routing considerably in message overhead. The reason that trust-based protocols use slightly more message copies than connectivity-based routing protocols is that the path being selected by trust-based protocols may not be the most direct route in order to avoid selfish or malicious nodes. In summary, from Figures 3-5, we see that trust-based protocols can effectively trade off message overhead (Figure 5) and message delay (Figure 4) for a significant gain in message delivery ratio (Figure 3) over connectivity-based routing protocols.

## 7. Conclusion

In this paper, we have proposed and analyzed a class of trust-based routing protocols in MANET DTNs. The most salient feature of our protocol is that we consider not only connectivity (QoS trust) but also honesty and unselfishness (social trust) properties into a composite trust metric for decision making in DTN routing dynamically. We formally proved that our protocol is resilient against whitewashing, bad-mouthing, and good-mouthing attacks by malicious nodes. We further substantiated the claim with numerical results demonstrating that a malicious node will never attain trustworthy status. Our performance analysis results demonstrate that by properly selecting weights associated with QoS and social trust metrics for trust evaluation, our trust management protocols can achieve the ideal performance level in delivery ratio and delay obtainable by epidemic routing, especially as the percentage of malicious and selfish nodes increases. In particular, trust-based protocols that consider both social and QoS trust can effectively trade off message delay and message overhead for a significant gain in message delivery ratio over connectivity-based routing protocols.

In the future, we plan to investigate other forms of message passing such as multi-copy message forwarding and other forms of attacks by malicious nodes such as jamming, forgery, and DoS attacks. We also plan to consider other trust metrics such as technical competence, betweenness centrality, similarity, and social ties (strength) [6]. Another direction is to investigate the best ratio of $w_1$: $w_2$: $w_3$: $w_4$ or $\beta_1$: $\beta_2$ based on knowledge about the application context.

## References

[1] M. Aldebert, M. Ivaldi, and C. Roucolle, "Telecommunications Demand and Pricing Structure: an Economic Analysis," *Telecommunication Systems*, vol. 25, no. 1-2, Jan. 2004, pp. 89-115.

[2] J. Burgess, B. Gallagher, D. Jensen, and B.N. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking," *IEEE Infocom 2006*, Barcelona, Spain, April 2006, pp. 1-11.

[3] J.H. Cho, A. Swami and I.R. Chen, "Modeling and Analysis of Trust Management for Cognitive Mission-driven Group Communication Systems in Mobile Ad Hoc Networks," *7th IEEE/IFIP Int. Symp. Trusted Computing and Communications*, Vancouver, Canada, Aug. 2009.

[4] G. Ciardo, R.M. Fricks, J.K. Muppala and K.S. Trivedi, *Stochastic Petri Net Package Users Manual*, Department of Electrical Engineering, Duke University, 1999.

[5] E.M. Daly and M. Haahr, "The Challenges of Disconnected Delay Tolerant MANETs," *Ad Hoc Networks*, vol. 8, no. 2, March 2010, pp. 241-250.

[6] E.M. Daly and M. Haahr, "Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs," *IEEE Transactions on Mobile Computing*, vol. 8, no. 5, May 2009, pp. 606-621.

[7] M. Karaliopoulos, "Assessing the Vulnerability of DTN Data Relaying Schemes to Node Selfishness," *IEEE Communications Letters,* vol. 13, no. 12, 2009, pp. 923-925.

[8] E. Bulut, Z. Wang and B.K. Szymanski, "Impact of Social Networks on Delay Tolerant Routing," *IEEE Globecom 2009*, Hawaii, USA, Nov. 2009, pp. 1804-1809.

[9] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," *IEEE Infocom 2010*, San Diego, CA, March 2010, pp. 1-9.

[10] S. Jain, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," *ACM Computer Communication Review*, vol. 34, no. 4, Oct. 2004. pp. 145-158.

[11] S.C. Nelson, M. Bakht and R. Kravets, "Encounter-based Routing in DTNs," *IEEE Infocom 2009*, Rio De Janeiro, Brazil, Apr. 2009, pp.846-854.

[12] U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNs," *16th IEEE Conf. on Network Protocols*, Orlando, FL, USA, Oct. 2008, pp. 238-247.

[13] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks," Technical Report, Computer Science Department, Duke University, 2000.

[14] Z. Xu, et al. "SReD: A Secure Reputation-Based Dynamic Window Scheme for Disruption-Tolerant Networks," *IEEE Military Communications Conf.*, Oct. 2009, pp. 1-7.

[15] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks", *IEEE Transactions on Vehicular Technology*, vol. 58, no. 8, Oct. 2009, pp. 4628-4638.